https://doi.org/10.31891/2219-9365-2025-83-49
УДК 004

ПЕТЛЯК Наталія
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
ТОВТ Растіслав
Хмельницький національний університет
tovtrastik1@gmail.com
КОБИЛЯНСЬКИЙ Іван
Хмельницький національний університет
vedirwan@gmail.com
ОЛІЙНИК Володимир
Хмельницький національний університет
olivolodumur357@gmail.com

ДЕСКРИПТОРНА МОДЕЛЬ СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ В ОПЕРАЦІЙНИХ СИСТЕМАХ MICROSOFT WINDOWS

В роботі розглянуто дескрипторну модель системи контролю й управління доступом в операційних системах Windows, що базується на принципах формалізованого опису взаємодії суб'єктів і об'єктів доступу в рамках політик безпеки. Проведено аналіз архітектури системи контролю доступу Windows, включно з токенами доступу, ACL, SID, механізмами аудиту та доменним керуванням через Active Directory. Визначено актуальні загрози, типові помилки конфігурації, уразливості та надано пропозиції щодо вдосконалення механізмів контролю доступу на основі сучасних міжнародних стандартів інформаційної безпеки. Обґрунтовано доцільність впровадження контекстно-орієнтованого доступу, принципу Zero Trust та застосування інтелектуальних механізмів аналізу поведінки користувачів. Запропоновано напрямки подальших досліджень щодо інтеграції штучного інтелекту в управління доступом у Windows-середовищах.

Ключові слова: контроль доступу, дескрипторна модель, Windows, ACL, SID, Active Directory, Zero Trust, ISO/IEC 27001, управління привілеями, інформаційна безпека.

PETLIAK Natalia, TOVT Rastislav, KOBYLIANSKYI Ivan, OLIINYK Volodymyr
Khmelnytskyi National University

DESCRIPTOR MODEL OF ACCESS CONTROL AND MANAGEMENT SYSTEM IN MICROSOFT WINDOWS OPERATING SYSTEMS

The article examines the descriptor-based model of access control and management in Windows operating systems, focusing on the formalized description of interactions between subjects and objects under security policies. The study provides an in-depth analysis of the Windows access control architecture, including access tokens, security identifiers (SID), access control lists (ACL), auditing mechanisms, and centralized management via Active Directory. The research identifies current threats, common misconfigurations, and vulnerabilities, while outlining recommendations for improving access control mechanisms in alignment with international information security standards such as ISO/IEC 27001, ISO/IEC 27002, and NIST SP 800-207. The article highlights the importance of adopting context-aware access, the principle of least privilege, Zero Trust architecture, and user behavior analytics to address emerging risks in dynamic IT environments. Special attention is given to domain-based infrastructures, where Group Policy Objects (GPO) and advanced audit configurations enhance centralized governance but also introduce complexity and potential mismanagement risks. The advantages of the descriptor model are emphasized in terms of its suitability for formal verification, automated monitoring, and adaptation to risk-oriented approaches. Directions for future research include the integration of artificial intelligence techniques—particularly behavioral analytics and anomaly detection—into Windows access management, supporting real-time policy adaptation and proactive incident response. Such advancements will enable organizations to align security practices with global standards while ensuring the confidentiality, integrity, and availability of information assets in modern digital ecosystems.

Keywords: access control, descriptor model, Windows, ACL, SID, Active Directory, Zero Trust, ISO/IEC 27001, privilege management, information security.

Стаття надійшла до редакції / Received 01.08.2025
Прийнята до друку / Accepted 22.08.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Забезпечення цілісності, конфіденційності та доступності інформації в умовах стрімкого розвитку цифрових технологій потребує комплексного підходу до контролю і управління доступом до ресурсів обчислювального середовища. Однією з найпоширеніших платформ, що забезпечують виконання обчислювальних задач у корпоративних і державних структурах, є операційні системи (ОС) сімейства Windows. Саме тому актуальність дослідження механізмів управління доступом у цих ОС набуває особливого значення, оскільки порушення механізмів авторизації та автентифікації безпосередньо впливають на рівень інформаційної безпеки організацій.

У статті здійснено аналіз принципів функціонування системи контролю доступу в ОС Windows, визначено складові елементи дескрипторної моделі такої системи, а також представлено концепцію її побудови з урахуванням положень національних (ДСТУ) та міжнародних (ISO/IEC) стандартів. Також розглянуто проблеми реалізації доступу до об'єктів та суб'єктів у рамках моделей мандатного, дискреційного і рольового контролю.

Теоретичні основи управління доступом

Система управління доступом (СУД) в ОС являє собою інтегрований комплекс технічних, програмних та адміністративних засобів, основною метою якого є регламентація прав доступу користувачів до інформаційних ресурсів відповідно до встановлених політик безпеки. У контексті забезпечення інформаційної безпеки вона виконує функцію щодо дотримання конфіденційності, цілісності та доступності даних у цифрових середовищах.

Відповідно до положень міжнародних стандартів ISO/IEC 27001:2022 та ISO/IEC 27002:2022, ефективна СУД повинна забезпечувати комплексне функціонування механізмів ідентифікації та автентифікації суб’єктів, контроль їхніх повноважень шляхом авторизації дій над ресурсами, ведення обліку фактів доступу з метою аудиту, а також захист та збереження конфігурацій політик безпеки в актуальному стані [1-3]. Саме ці механізми становлять методологічну основу сучасної моделі управління доступом, яка в умовах цифрової трансформації організацій має адаптуватися до нових викликів, пов’язаних із розподіленими системами, хмарними обчисленнями та мобільністю користувачів.

Політики доступу в сучасних інформаційних системах визначаються як множина правил, що формалізують, хто, за яких умов і до яких об'єктів може здійснювати певні дії. Ці політики реалізуються на основі певних моделей контролю доступу, кожна з яких відображає певну концепцію безпеки [4]. У класичних системах застосовуються дискреційні, мандатні та рольові моделі. У дискреційній моделі власник ресурсу самостійно визначає права доступу інших суб’єктів, а мандатний підхід базується на централізовано визначених політиках, що не підлягають зміні на рівні користувача [5]. Рольова модель, своєю чергою, ґрунтується на призначенні прав не окремим користувачам, а їхнім ролям у межах організаційної структури.

У реальних умовах експлуатації ОС Windows, особливо у серверних версіях, реалізовано гібридний підхід, що поєднує елементи дискреційної та ролевої моделей. Це забезпечує високу гнучкість і масштабованість у керуванні доступом [6-7]. Зокрема, реалізація управління здійснюється за допомогою списків контролю доступу (ACL), які містять записи, що визначають дозволені або заборонені дії для конкретних суб’єктів [8]. Ці записи асоційовані з унікальними ідентифікаторами безпеки (SID), що надаються користувачам і групам у середовищі Windows. Під час автентифікації система створює спеціальні токени доступу, які містять інформацію про обліковий запис користувача, його групову приналежність, делеговані привілеї та інші атрибути, необхідні для прийняття рішень щодо дозволу або заборони дій над ресурсами.

Вагомим елементом централізованого управління виступає Active Directory, що дозволяє формувати доменну інфраструктуру, здійснювати централізоване адміністрування облікових записів, застосовувати групові політики та делегувати адміністративні функції у великих корпоративних мережах [9]. З огляду на швидку еволюцію загроз і необхідність гнучкої реакції систем безпеки, дедалі більшого значення набувають моделі контекстно-орієнтованого управління доступом. Такий підхід враховує додаткові параметри середовища, зокрема місцезнаходження, тип пристрою, час доступу, поведінкові шаблони користувача, що дозволяє приймати гнучкіші рішення в умовах змінного ризику.

Крім того, важливим концептуальним зрушенням у сфері контролю доступу є перехід до архітектури нульової довіри (Zero Trust Architecture), яка заперечує традиційний поділ на "довірену" внутрішню мережу та "недовірене" зовнішнє середовище. Замість цього кожен запит до ресурсу розглядається як потенційно шкідливий, незалежно від походження, і повинен бути перевірений через механізми аутентифікації, авторизації та моніторингу в реальному часі [10-11].

Таким чином, система контролю доступу в ОС Windows являє собою багаторівневу структуру, яка вимагає регулярного удосконалення, ретельного налаштування та безперервного аудиту. Вона повинна бути інтегрована у загальну політику інформаційної безпеки організації та відповідати актуальним міжнародним стандартам. У контексті переходу до цифрових платформ і хмарних технологій постає необхідність у модернізації класичних підходів до управління доступом шляхом їх поєднання з інтелектуальними системами моніторингу, автоматизованого реагування на інциденти та поведінкового аналізу. Це дозволить забезпечити не лише відповідність нормативним вимогам, а й реальну ефективність захисту інформаційних активів організації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Система управління доступом в ОС Windows реалізується через багаторівневу архітектуру, що інтегрує компоненти автентифікації, авторизації, контролю привілеїв і аудиту дій користувачів. Ідентифікація користувачів здійснюється на основі облікових записів, які можуть бути локальними або доменними, а процес автентифікації базується на механізмах Active Directory та протоколі Kerberos. Після проходження

автентифікації система створює access token, який містить SID користувача, ідентифікатори груп та перелік наданих прав. Саме цей токен визначає можливості суб'єкта під час виконання подальших операцій у системі. Доступ до файлів, реєстру, служб і мережевих ресурсів регламентується ACL, що складаються з Access Control Entries (ACE), кожен із яких фіксує набір дозволених чи заборонених дій для певного користувача, групи або процесу [12]. Центральну роль у забезпеченні функціонування механізмів безпеки відіграють служби Local Security Authority (LSA), Security Account Manager (SAM) і, у випадку використання доменної інфраструктури, служби Active Directory. Вони забезпечують узгоджену обробку облікових записів, політик безпеки, токенів і аудиторських налаштувань. Крім того, система дозволяє реалізовувати контроль привілеїв за допомогою механізмів групової політики, які адміністратори можуть налаштовувати відповідно до внутрішніх вимог організації.

З метою забезпечення підзвітності та контролю порушень, у ОС Windows впроваджено потужну систему аудиту, що базується на підсистемі Windows Event Log та налаштуваннях політик аудиту. Це дає змогу фіксувати дії користувачів, зміни прав доступу, спроби несанкціонованого доступу та інші важливі події безпеки, що є невід'ємною частиною процесу моніторингу інформаційної безпеки в середовищі Windows [13-14].

Формалізація процесів управління доступом в ОС Windows можлива за допомогою дескрипторної моделі, яка дозволяє структурувати взаємозв'язки між суб'єктами, об'єктами, діями та політиками доступу на рівні математичного представлення. Така модель має на меті забезпечити уніфікований підхід до аналізу ефективності реалізації контролю доступу в різних середовищах, а також дозволяє порівнювати структури безпеки між платформами. Основними елементами цієї моделі виступають суб'єкти доступу, якими можуть бути як користувачі, так і групи чи прикладні процеси, та об'єкти, до яких належать файли, каталоги, ключі реєстру, мережеві шари, служби, апаратні компоненти тощо. Політики доступу визначають набір правил, які вказують, які дії дозволено або заборонено здійснювати над конкретними об'єктами для певних суб'єктів. У цій моделі також враховуються системні атрибути, такі як SID, ACL, налаштування облікових записів та конфігурації групових політик (GPO).

Перевага дескрипторної моделі полягає в її придатності до формального верифікаційного аналізу та автоматизації моніторингу стану безпеки, що особливо важливо в умовах швидкої зміни середовища IT-інфраструктури. У разі необхідності модель може бути адаптована до умов динамічного управління доступом, зокрема до контекстно-чутливих або ризик-орієнтованих підходів, які є основою сучасних Zero Trust моделей.

У доменних середовищах, де керування доступом здійснюється через інфраструктуру Active Directory, архітектура системи безпеки ускладнюється багаторівневою структурою ієрархій. Доменні дерева, ліси, організаційні одиниці (OU) та об'єкти політик формують складну екосистему керування привілеями, делегуванням повноважень і централізованою аутентифікацією. Контроль доступу в такому середовищі регламентується за допомогою об'єктів групової політики (Group Policy Objects, GPO), що дозволяють централізовано визначати та застосовувати конфігурації доступу до ресурсів і служб. Особливістю такої моделі є можливість налаштування доступу через механізми фільтрації безпеки (Security Filtering), а також фільтрації за допомогою WMI-запитів, що враховують контекст користувача або пристрою, такі як тип обладнання, версія ОС, мережеве підключення або стан оновлення. Завдяки такому підходу політики контролю доступу набувають динамічності й контекстної гнучкості, що узгоджується з ризик-орієнтованими методами управління. Для аудиту у доменних середовищах використовується Advanced Audit Policy Configuration, яка забезпечує детальне відстеження подій — від спроб входу до змін у параметрах безпеки. Журнали подій Windows у поєднанні з рішеннями на кшталт Microsoft Sentinel чи Defender for Identity створюють можливості для кореляції інцидентів і побудови поведінкових моделей користувачів. Застосування таких механізмів повністю відповідає вимогам стандарту ДСТУ ISO/IEC 27001 щодо забезпечення підзвітності, виявлення інцидентів та впровадження засобів реагування. Таким чином, у доменних середовищах Windows спостерігається синергія між структурним, політичним та поведінковим контролем доступу, що створює передумови для впровадження більш просунутих концепцій безпеки, таких як Zero Trust Architecture, де довіра формується не на основі розташування в мережі, а виключно на основі ідентичності, контексту та атестації пристроїв.

Попри багаторівневу структуру захисту та використання механізмів контролю доступу, ОС Windows залишається вразливою до цілого спектра атак, пов'язаних із компрометацією компонентів системи автентифікації, авторизації та управління привілеями. Однією з найбільш поширених загроз є ескалація привілеїв, яка відбувається шляхом використання слабко захищених або некоректно налаштованих списків контролю доступу. Внаслідок цього зловмисник може отримати розширені повноваження в системі, обійти обмеження або навіть здійснити контроль над критично важливими ресурсами. Не менш критичними є ситуації, коли політики безпеки в рамках GPO або конфігурації груп у середовищі Active Directory мають прогалини або надмірні дозволи, що відкриває вікно можливостей для атаки зсередини або автоматизованих атак через експлойти.

Серед сучасних способів компрометації автентифікаційних даних виділяють техніки Pass-the-Hash та Pass-the-Ticket. Вони дають змогу зловмиснику проходити перевірку в системі без введення справжнього

пароля [15]. Додаткові ризики становлять методи обходу User Account Control (UAC) та маніпуляції з токенами доступу, завдяки яким процеси можуть функціонувати з адміністративними правами, що підриває захищеність механізмів ідентифікації.

Для протидії подібним вектором атак сучасні концепції інформаційної безпеки передбачають впровадження принципу найменших привілеїв (PoLP), згідно з яким користувач або процес має отримувати лише той обсяг доступу, який є необхідним для виконання конкретних функцій. Окрім цього, велике значення має постійний аудит прав доступу, виявлення відхилень у конфігурації системи та аналіз історії подій безпеки. До практичних інструментів, що дозволяють реалізувати такі функції, належать платформи оцінки відповідності конфігурацій (SCA), системи поведінкового аналізу доступу на кшталт Microsoft Defender for Identity, а також спеціалізовані засоби графового аналізу, зокрема BloodHound, які дозволяють виявляти приховані вектори ескалації прав у складних інфраструктурах.

В умовах зростаючої складності інформаційних систем та розширення периметру корпоративних мереж, традиційні моделі управління доступом потребують трансформації відповідно до принципів гнучкості, адаптивності та контекстної обізнаності. Одним із ключових напрямів розвитку є включення до дескрипторної моделі управління доступом змінних контексту, таких як географічне розташування користувача, час доби, тип пристрою, рівень оновлення ОС або стан антивірусного захисту. Це дозволяє перейти від статичних до динамічних механізмів контролю, де рішення щодо надання або обмеження доступу приймається з урахуванням поточних умов і ризиків. Ще одним важливим аспектом модернізації є впровадження поведінкової аналітики, яка забезпечує динамічне призначення ролей та прав доступу на основі виявлення аномалій у поведінці користувача. Такий підхід передбачає постійне оновлення моделей доступу в реальному часі, що знижує ризик компрометації системи навіть у випадку витоку облікових даних.

Централізований аудит, що здійснюється за допомогою інтеграції з системами управління подіями та інформацією безпеки (SIEM), дозволяє створити єдину інформаційну базу про всі інциденти, спроби доступу та зміни в конфігурації системи безпеки. Це відкриває можливості не лише для оперативного реагування на інциденти, а й для стратегічного планування заходів щодо підвищення рівня безпеки. Крім того, автоматизація таких процесів, як зміна паролів, управління криптографічними ключами та динамічне оновлення токенів доступу, дозволяє знизити залежність від людського фактора та мінімізувати ризик експлуатації старих облікових даних.

Значну роль у підвищенні стійкості моделі управління доступом відіграє впровадження двофакторної автентифікації, що забезпечує додатковий рівень захисту ідентифікаційної інформації. Зазначені вектори атак актуалізують принципи Zero Trust Architecture, де жоден користувач чи процес не розглядається як довірений за замовчуванням, незалежно від його місця у мережі чи попередньої історії автентифікацій. Згідно з рекомендаціями NIST SP 800-207, кожна транзакція в системі повинна проходити повторну перевірку і відповідати актуальним політикам доступу, що значно підвищує адаптивність системи до нових загроз.

Отже, подальший розвиток дескрипторної моделі управління доступом має ґрунтуватися на принципах контекстної обізнаності, адаптивності, поведінкової аналітики та автоматизованого аудиту, що відповідає викликам сучасної кібербезпеки.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У роботі подано дескрипторну модель системи контролю доступу в ОС Windows. Вона враховує особливості архітектури ОС та положення сучасних стандартів інформаційної безпеки, формуючи основу для адаптивних політик управління. Використання формалізованого підходу дозволяє підвищити ефективність контролю, уніфікувати процедури аудиту доступу, а також забезпечити відповідність вимогам ДСТУ ISO/IEC 27001:2022. У майбутньому доцільно зосередити дослідницькі зусилля на розробці моделей адаптивного доступу із застосуванням методів штучного інтелекту, зокрема алгоритмів поведінкової аналітики, а також на інтеграції цих моделей у корпоративні засоби захисту (EDR, XDR, SIEM).

Література

1. ДСТУ ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – Чинний з 01.01.2023.

2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.

3. ISO/IEC 27005:2022. Information security risk management.

4. Капелюшна Т., Мужанова Т., Берестяна Т., Голобородько С., Примаченко Д. Механізм управління доступом до інформаційних ресурсів на підприємстві // Кібербезпека: освіта, наука, техніка. – 2025. – Т. 3, № 27. – С. 205–219. – DOI: 10.28925/2663-4023.2025.27.743.

5. Aftab M. U., Hamza A., Oluwasanmi A., Nie X., Sarfraz M. S., Shehzad D., Qin Z., Rafiq A. Traditional and Hybrid Access Control Models: A Detailed Survey // Security and Communication Networks. – 2022. – Article ID 1560885. – 12 p. – DOI: 10.1155/2022/1560885.

6. Keyogeg B., Thompson M., Dawson G., et al. Automated Detection of Ransomware in Windows Active Directory Domain Services Using Log Analysis and Machine Learning // Authorea. – 2024. – 1 Oct. – DOI: 10.22541/au.172779663.36925703/v1.

7. Syed A. A. M. Zero Trust Security in Hybrid Cloud Environments: Implementing and Evaluating Zero Trust Architectures in AWS and On-Premise Data Centers // International Journal of Emerging Trends in Computer Science and Information Technology. – 2024. – Vol. 5, No. 2. – P. 42–45. – URL: https://ijetcsit.com (дата звернення: 24.07.2025).

8. Microsoft. Access control list [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/access-control-list (дата звернення: 24.07.2025).

9. Microsoft. Active Directory Domain Services overview [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата звернення: 24.07.2025).

10. Guo X., Xian H., Feng T., Jiang Y., Zhang D., Fang J. An intelligent zero trust secure framework for software defined networking // PeerJ Computer Science. – 2023. – Vol. 9. – e1674. – DOI: 10.7717/peerj-cs.1674.

11. Microsoft. Zero Trust [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/zero-trust (дата звернення: 24.07.2025).

12. McDonald G., Papadopoulos P., Pitropakis N., Ahmad J., Buchanan W. J. Ransomware: Analysing the Impact on Windows Active Directory Domain Services // Sensors. – 2022. – Vol. 22, No. 3. – P. 953. – DOI: 10.3390/s22030953.

13. Pulls E. Efficient Windows logging for Incident Response: A comparison of logging strategies for malware and threat detection: Dissertation. – Stockholm: KTH Royal Institute of Technology, 2024.

14. Mailewa A., Rozendaal K. A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study // Advances in Technology. – 2022. – Vol. 2, No. 3. – P. 291–321. – DOI: 10.31357/ait.v2i3.5584.

15. Moric Z., Dakic V., Redzepagic J., Otocan F. Penetration Testing and Exploitation of Active Directory Configuration Vulnerabilities // Proc. of the 4th Intelligent Cybersecurity Conference (ICSC). – Valencia, Spain, 2024. – P. 118–126. – DOI: 10.1109/ICSC63108.2024.10895772.

References

1. DSTU ISO/IEC 27001:2022. Information technologies. Security methods. Information security management systems. Requirements. – Effective from 01.01.2023.

2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.

3. ISO/IEC 27005:2022. Information security risk management.

4. Kapeliushna T., Muzhanova T., Berestiana T., Holoborodko S., Prymachenko D. Mekhanizm upravlinnia dostupom do informatsiinykh resursiv na pidpryiemstvi [Access Control Mechanism for Information Resources at the Enterprise] // Cybersecurity: Education, Science, Technology. – 2025. – Vol. 3, No. 27. – P. 205–219. – DOI: 10.28925/2663-4023.2025.27.743.

5. Aftab M. U., Hamza A., Oluwasanmi A., Nie X., Sarfraz M. S., Shehzad D., Qin Z., Rafiq A. Traditional and Hybrid Access Control Models: A Detailed Survey // Security and Communication Networks. – 2022. – Article ID 1560885. – 12 p. – DOI: 10.1155/2022/1560885.

6. Keyogeg B., Thompson M., Dawson G., et al. Automated Detection of Ransomware in Windows Active Directory Domain Services Using Log Analysis and Machine Learning // Authorea. – 2024. – 1 Oct. – DOI: 10.22541/au.172779663.36925703/v1.

7. Syed A. A. M. Zero Trust Security in Hybrid Cloud Environments: Implementing and Evaluating Zero Trust Architectures in AWS and On-Premise Data Centers // International Journal of Emerging Trends in Computer Science and Information Technology. – 2024. – Vol. 5, No. 2. – P. 42–45. – URL: https://ijetcsit.com (accessed: 24.07.2025).

8. Microsoft. Access control list [Electronic resource]. – Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/access-control-list (accessed: 24.07.2025).

9. Microsoft. Active Directory Domain Services overview [Electronic resource]. – Available at: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (accessed: 24.07.2025).

10. Guo X., Xian H., Feng T., Jiang Y., Zhang D., Fang J. An intelligent zero trust secure framework for software defined networking // PeerJ Computer Science. – 2023. – Vol. 9. – e1674. – DOI: 10.7717/peerj-cs.1674.

11. Microsoft. Zero Trust [Electronic resource]. – Available at: https://www.microsoft.com/uk-ua/security/business/zero-trust (accessed: 24.07.2025).

12. McDonald G., Papadopoulos P., Pitropakis N., Ahmad J., Buchanan W. J. Ransomware: Analysing the Impact on Windows Active Directory Domain Services // Sensors. – 2022. – Vol. 22, No. 3. – P. 953. – DOI: 10.3390/s22030953.

13. Pulls E. Efficient Windows logging for Incident Response: A comparison of logging strategies for malware and threat detection: Dissertation. – Stockholm: KTH Royal Institute of Technology, 2024.

14. Mailewa A., Rozendaal K. A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study // Advances in Technology. – 2022. – Vol. 2, No. 3. – P. 291–321. – DOI: 10.31357/ait.v2i3.5584.

15. Moric Z., Dakic V., Redzepagic J., Otocan F. Penetration Testing and Exploitation of Active Directory Configuration Vulnerabilities // Proceedings of the 4th Intelligent Cybersecurity Conference (ICSC). – Valencia, Spain, 2024. – P. 118–126. – DOI: 10.1109/ICSC63108.2024.10895772.